Manuale del sistema di Gestione del Trattamento dei Dati Personali ai sensi del Regolamento UE 2016/679 e D.LGS. 196/03 come modificato dal D.LGS. 101/2018

1. PREMESSA E SCOPO DEL MANUALE

Scopo del presente manuale è di regolamentare l'organizzazione complessiva della privacy, sia interna sia esterna, in modo da garantire che il trattamento dei dati personali avvenga secondo le norme del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 e del Codice Privacy (D.Lgs. 196/2003), come aggiornato a cura del D. Lgs. 101/2018, nel rispetto della dignità umana, dei diritti e delle libertà fondamentali della persona.

Appare dunque opportuno redigere e strutturare un documento volto a:

1) individuare la tipologia di dati personali, pertinenti a persone fisiche, trattati da **Bioware S.r.l.** e stabilire le corrette procedure per ciascun tipo di trattamento (finalità, responsabilità, modalità e durata);
2) descrivere le misure di sicurezza organizzative, fisiche e logiche che **Bioware S.r.l.** predispone nel ruolo di Titolare del trattamento dei dati in modo da prevenire, mitigare, eliminare o trasferire, comunque ridurre al minimo i rischi derivanti dal trattamento dei dati personali, con particolare attenzione a quelli di natura sensibile e ultra sensibile, all'interno della nuova categoria, dei dati c.d. "particolari", delineata e disciplinata dal Regolamento UE 2016/679.
   Il documento illustra le misure già in atto e si propone di ottimizzare le procedure necessarie alla corretta esecuzione di quanto previsto dalla legge, in un'ottica di miglioramento continuo, anche sulla base delle evoluzioni tecnologiche (segnatamente nel comparto dell'informatica).
   Si specifica che tale documento, unitamente agli allegati che compongono il modello organizzativo in materia di "privacy", rappresenta le politiche organizzative e gestionali, nonché di valutazione dei rischi specifici.

Il presente Manuale è predisposto alla luce della vigente normativa di riferimento in materia di protezione dei dati personali.

In primo luogo, in ambito nazionale, il Manuale si adegua al D. Lgs. 6 aprile 2003, n. 196 (d'ora in avanti "D. lgs. 196/2003") e s.m.i. nonché ai pertinenti provvedimenti emanati dal Garante per la protezione dei dati personali (d'ora in avanti "Garante privacy").
Peraltro si segnala che il 24 maggio 2016 è entrato in vigore il Regolamento UE 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 (d'ora in avanti "Regolamento UE") in materia di protezione

dei dati personali.

Tale Regolamento è obbligatorio a far data dal 25 maggio 2018; pertanto **Bioware S.r.l.** provvede con il presente documento alla strutturazione ed organizzazione del proprio sistema di gestione della privacy, garantendo la conformità del sistema medesimo alla normativa europea e del recente Decreto Legislativo 10 agosto 2018, n. 101, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)" (in G.U. 4 settembre 2018 n.205).

Le revisioni periodiche del sistema saranno occasione, fra l'altro, per l'ulteriore adeguamento alle previsioni obbligatorie del Regolamento UE e alle eventuali e future normative nazionali.

2. NORMATIVA DI RIFERIMENTO

- ✓ *Decreto Legislativo 30 giugno 2003, n. 196,* modificato dal Decreto Legislativo 10 agosto 2018 n. 101 – Codice Privacy;
- ✓ *Allegato B* – Disciplinare Tecnico in materia di misure minime di sicurezza (***abrogato dall'articolo 27, comma 1, lett. d), del decreto legislativo 10 agosto 2018, n. 101*** *- Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE - regolamento generale sulla protezione dei dati) **(**l'allegato B è stato abrogato espressamente dal D. Lgs. 101/2018, pertanto le misure minime di sicurezza non sono più disciplinate; tuttavia, si ritiene utile considerarle alla stregua di "soglia minima" di sicurezza al di sotto della quale non si può scendere, in ogni caso, in ottica di accountability);*
- ✓ *Provvedimento del Garante 23 novembre 2006* – Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati;
- ✓ *Provvedimento del Garante 19 giugno 2008* - Semplificazioni di taluni adempimenti in ambito pubblico e privato rispetto a trattamenti per finalità amministrative e contabili;
- ✓ *Provvedimento del Garante 1 marzo 2007* – Linee guida del garante per posta elettronica e internet;
- ✓ *Provvedimento del Garante 27 novembre 2008* – Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema ***(*tale elemento non viene espressamente richiamato dal Regolamento UE 2016/679 tuttavia si ritiene il provvedimento pienamente compatibile con il Regolamento predetto e costituisce una delle misure di sicurezza adeguate*);
- ✓ ***Provvedimento del Garante 10 dicembre 2009* - Amministratori di sistema: precisazioni del**

Garante (cfr. sopra);

- ✓ Vademecum del Garante "La privacy dalla parte dell'impresa" – maggio 2013;
- ✓ *Provvedimento del Garante 13 luglio 2016* - Trattamento di dati personali dei dipendenti mediante posta elettronica e altri strumenti di lavoro;
- ✓ Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

3. DEFINIZIONI

L'art. 4 del Regolamento UE 2016/679 riporta le seguenti definizioni**:**

- ***Trattamento*** – qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- ***Dato personale*** – qualsiasi informazione riguardante una persona fisica, identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata direttamente o indirettamente, con particolare riferimento un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- ***Archivio*****:** qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico (la definizione si ritiene integrante della definizione nazionale di "Banca dati");
- ***Profilazione*****:** qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
- ***Pseudonimizzazione*****:** il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
- ***Destinatario***: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi.
- ***Terzo***: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile.
- ***Categorie particolari di dati***: i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni

religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale, nonché i dati genetici ed i dati biometrici (cfr. *art. 9 Regolamento Ue 2016/679 e art. 2 – septies del D. Lgs. 196/03 come modificato dal D. Lgs. 101/2018*). *(Dati giudiziari)* ora "**trattamento dei dati personali relativi a reati e condanne penali**"* (cfr. *art. 10 Regolamento Ue 2016/679*) – i dati personali idonei a rivelare le condanne penali, i reati e connesse misure di sicurezza

- ***Titolare del trattamento***: la persona fisica o giuridica, la autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
- ***Responsabile del trattamento***: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento (cfr. art. 28 e 29 del Regolamento Ue 2016/679 e la figura del "designato" ai sensi del d. lgs. 101/2018).
  (Incaricati) – (cfr. art. 4 D.Lgs. 196/03) le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile (tale indicazione non è stata ripresa dal Regolamento Ue 2016/679 e neppure dal D. Lgs. 101/2018 che ha modificato il D. Lgs. 196/2003 - si fa ora riferimento alle **"persone autorizzate"** ***art. 4 par.1, n. 10 Regolamento UE 2016/679*** e a **"coloro che agiscono sotto l'autorità"** del titolare o del responsabile ***art. 29 Regolamento UE 2016/679***")
  (Interessato) – (cfr. definizione di dato personale sopra riportata) la persona fisica, cui si riferiscono i dati personali (Comma così modificato dall'art. 40, comma 2, lettera b), del decreto legge 6 dicembre 2011, n. 201, convertito, con modificazioni, dalla legge 22 dicembre 2011, n. 214)
- ***Consenso dell'interessato***: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
- ***Violazione dei dati personali***: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
- ***Dati genetici***: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
- ***Dati biometrici***: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
- ***Dati relativi alla salute:*** i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

- ***Stabilimento principale:*** **a)** per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi di trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale; **b)** con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede l'amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha una amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'unione in cui sono condotte le principali attività di trattamento nella misura in cui tale responsabile è soggetto ad obblighi specifici ai sensi del presente regolamento;
- ***Rappresentante***: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'art. 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;
- ***Impresa***: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;
- ***Gruppo imprenditoriale***: un gruppo costituito da un'impresa controllante e delle imprese da questa controllate;
- ***Norme vincolanti di impresa***: le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;
- ***Autorità di controllo***: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'art. 51 del Regolamento UE 2016/679.

Per completezza di informazione nel passaggio dalla precedente normativa a quella attualmente vigente di seguito si riportano ulteriori definizioni non più contenute nel Regolamento UE 2016/679.

- ***Comunicazione****:* il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- ***Diffusione:*** il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- ***Dato anonimo:*** il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
- ***Blocco****:* la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;
- ***Banca di dati***: qualsiasi complesso organizzato di dati personali, ripartito in una o

più unità dislocate in uno o più siti;

- ***Garante***: l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675.
- ***Misure minime****:* il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31 d. lgs. 193/2006;
- ***Strumenti elettronici:*** gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;
- ***Autenticazione informatica:*** l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;
- ***Credenziali di autenticazione:*** i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l' autenticazione informatica;
- ***Parola chiave****:* componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;
- ***Profilo di autorizzazione****:* l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;
- ***Sistema di autorizzazione****:* l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente;
- ***Violazione di dati personali:*** violazione della sicurezza che comporta anche accidentalmente la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o comunque elaborati nel contesto della fornitura di un servizio di comunicazione accessibile al pubblico.

4. PRINCIPI GENERALI SUL TRATTAMENTO DEI DATI PERSONALI

Il trattamento dei dati personali secondo le modalità stabilite nel presente manuale si ispira ai seguenti principi e criteri di cui al CAPO II del Regolamento UE 2016/679, in particolare agli artt. 5, 6, 7, 8, 9, 10 e 11.

Art. 5 – Principi applicabili al trattamento di dati personali

a) Liceità, correttezza e trasparenza

b) Limitazione della finalità (raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non vi sia incompatibilità con tali finalità)

c) Minimizzazione dei dati (adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati

- ***Principio di necessità (ovvero della minima gestione necessaria degli altrui dati personali*** *- ciò significa che l'utilizzazione di dati personali e di dati identificativi deve essere ridotta al minimo, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante dati anonimi (pseudonimizzazione) o mediante una minore quantità di dati acquisiti e/o pubblicati (si devono acquisire e trattare i soli dati strettamente necessari per le finalità dichiarate, evitando di acquisire quelli sovrabbondanti; se sono sufficienti dati personali semplici, non devono essere acquisiti dati sensibili o giudiziari). Il trattamento di dati personali, inoltre, deve essere contenuto nei limiti dell'indispensabile quanto a durata (i dati divenuti inutili devono essere cancellati –* ***principio della durata del trattamento****) e accessibilità (i dati non devono essere diffusi*

e/o pubblicati e/o comunicati a terzi se non nei limiti dello stretto necessario, oltre che, ovviamente, nel rispetto dei limiti di legge; lo stesso trattamento interno deve avvenire coinvolgendo il minor numero di incaricati possibile);

d) Esattezza (esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati)

e) Limitazione della conservazione

f) Integrità e riservatezza

g) **Principio di responsabilizzazione (*accountability - art. 5 par. 2 Regolamento UE 2016/679)***

Il Regolamento UE richiede che il Titolare del trattamento adotti misure tecniche e organizzative che siano non solo adeguate a garantire che il trattamento sia conforme al Regolamento (più in generale, che esso sia conforme alla normativa vigente), ma anche idonee a dimostrare tale idoneità nei confronti di tutti gli stakeholders.
A tale principio risponde la scelta aziendale di predisporre un apposito sistema di gestione della privacy, racchiuso nel presente Manuale, secondo modalità già note nel campo dei modelli organizzativi ex d. lgs. 231/2001, nel campo dei sistemi qualità e in generale nei sistemi di gestione di specifici aspetti dell'attività di impresa (sicurezza sul lavoro, ambiente ecc.)

Tra gli obblighi generali dettati dal Regolamento Ue 2016/679 vi sono i seguenti:

h) Privacy by design e by default

Il Regolamento UE (art. 25) dispone che il Titolare del trattamento dei dati mete in atto misure tecniche e organizzative adeguate, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso.
Il Titolare mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento.

5. COMPITI E RESPONSABILITÀ

Titolare del trattamento è:

- **Bioware S.r.l.,** considerata nel suo complesso di ente giuridico. All'azienda spetta esercitare il potere decisionale sulle finalità e sulle modalità del trattamento dei dati personali.

Il Titolare è tenuto ad adottare misure tecniche e organizzative adeguate per garantire ed essere in grado di dimostrare che il trattamento effettuato è conforme alla normativa.
Tale potere è esercitato attraverso l'adozione del presente sistema secondo le regole organizzative interne dell'ente.
Ogni ulteriore modifica o integrazione del sistema richiede l'adozione delle medesime modalità.

Il Titolare ha l'obbligo di identificare le figure aziendali interne in grado di assicurare una corretta adozione degli adempimenti richiesti.
Le figure previste dal Codice privacy (Regolamento UE 2016/679), oltre al Titolare sono:

- Il **Responsabile del trattamento** - È colui che tratta dati personali per conto del titolare del trattamento.

  Quando è soggetto esterno deve essere contrattualizzato con indicazioni dettagliate di quanto deve eseguire per conto del titolare.

  Quando è soggetto interno alla struttura aziendale viene chiamato "designato" **(**art. 28 regolamento UE e art. 2 *quaterdecies* D.Lgs. 101/2018 - ***con l'entrata in vigore del d. lgs. 101/2018 si parla di "designato" –*** *possono essere anche più di uno*). Collabora con il Titolare alla corretta adozione degli adempimenti privacy in azienda (ha compiti specifici ed è individuato in relazione al suo ruolo gerarchico interno).

  I compiti del Responsabile interno del trattamento sono:

  - Elaborare e predisporre ogni documento necessario per il corretto adempimento previsto dalla legge, ad esempio l'invio di informative e la richiesta di consenso dell'interessato, ove necessario, anche in relazione all'eventuale trasferimento all'estero dei dati ed alla loro comunicazione a terzi in considerazione delle ordinarie esigenze della Società.

  - Assicurare che il trattamento dei dati si svolga nel rispetto dei diritti, delle libertà fondamentali e della dignità delle persone fisiche, con particolare riferimento alla riservatezza ed all'identità personale.

  - Individuare gli incaricati (i **soggetti autorizzati a trattare dati**) e fornire loro le necessarie istruzioni scritte.

  Il Responsabile deve essere individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza (art. 29, co. 2 d. lgs. 196/2003 – 32 Regolamento UE). Tale profilo è accentuato dalle previsioni del Regolamento UE, secondo cui, qualora un trattamento debba essere effettuato **per conto** del Titolare del trattamento, quest'ultimo ricorre unicamente a Responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del regolamento e garantisca la tutela dei diritti dell'interessato (art. 28, co. 1 Regolamento UE).

  La designazione del Responsabile (interno) del trattamento è facoltativa. La designazione avviene con una lettera di incarico (cfr. "***altro atto giuridico…" art. 28 paragrafo 6 del Regolamento Ue)*** in cui sono specificate:

  1. le responsabilità e i compiti che competono a ciascun Responsabile,
  2. la durata del trattamento,
  3. la natura e la finalità del trattamento,

4. il tipo di dati personali e le categorie di interessati,
5. gli obblighi e i diritti del titolare del trattamento,

   e che dovrà essere controfirmata dall'interessato per accettazione.

In occasione dell'accettazione deve essere messa a disposizione del Responsabile, che ne firma l'originale sull'apposito foglio firme per presa visione, una copia della presente disciplina interna di gestione della privacy.

La completa informazione sul presente sistema di gestione, così trasmessa, soddisfa l'obbligo di istruzione da parte del Titolare del trattamento a norma dell'art. 29 Regolamento UE (*"il responsabile del trattamento … che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento"*).

Copia della lettera di nomina accettata deve essere conservata dal Titolare del trattamento in luogo sicuro.

Il Titolare, in relazione alle esigenze dell'azienda, potrà rivolgersi a un profilo professionale specializzato esterno oppure rivolgersi a una risorsa interna, purché siano rispettati i seguenti requisiti (stabiliti da **Bioware S.r.l.** in attuazione dei requisiti di esperienza, capacità e affidabilità):

- ✓ pregressa esperienza nel ruolo di Responsabile del trattamento, anche presso persone/enti diversi dal Titolare, per almeno due anni;
- ✓ in alternativa, il possesso di titoli di studio o specializzazione attinenti alla materia della privacy ovvero idonei a garantire, comunque, il pieno possesso della materia giuridica (ad es. consulenti privacy, avvocati);
- ✓ ovvero apposita formazione per almeno 8 ore complessive su un programma comprendente al minimo: esame del d. lgs. 196/2003 e s.m.i. (d. lgs. 101/2018) e del Regolamento UE sulla privacy; figure e responsabilità in materia di privacy; diritti dell'interessato e modalità di esercizio misure minime di sicurezza; esame del sistema di gestione interno della privacy.

Il Responsabile del trattamento non potrà ricorrere a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del Titolare del trattamento.

La nomina del Responsabile (interno) è a tempo indeterminato, salva decadenza per cessazione del rapporto di lavoro con il Responsabile (se dipendente), dimissioni del Responsabile o revoca da parte del Titolare del trattamento.

Il potere di revoca da parte del Titolare può essere esercitato in ogni momento e senza preavviso.

- ❖ **Vigilanza da parte del Titolare del Trattamento.**

Il Titolare del trattamento mantiene compiti di vigilanza nei confronti del Responsabile e inoltre garantisce che il Responsabile sia dotato degli strumenti necessari e opportuni – finanziari e di personale - per adempiere agli obblighi di legge.

La vigilanza del Titolare si realizza, in particolare, attraverso visite periodiche con cadenza almeno annuale

Le visite sono documentate da un **report**, firmato dal Titolare del trattamento e

controfirmato dal Responsabile.

Al momento dell'adozione del presente sistema **assume il ruolo di designato nel ruolo di Responsabile interno del Trattamento l'Ing. Barletta Massimiliano**.

a) Gli **Incaricati del trattamento (N.B.:** *il Regolamento Ue in verità non riporta la definizione di incaricato ma ad esso ci si riferisce, all'interno della definizione di "**terzo**", (art. **4 par. 1 n. 10 ….come …..persona autorizzata al trattamento dei dati** sotto l'autorità diretta del titolare o del responsabile . cfr. anche con art. 29 **..chiunque agisca sotto l'autorità del titolare o del responsabile e art. 2 quaterdecies D.Lgs. 101/2018**. Peraltro, stando all'articolato del Regolamento non è da escludere che ci si possa riferire anche a enti collettivi e non solo a persone fisiche*) - Sono coloro che materialmente gestiscono ed elaborano i dati e devono essere designati per iscritto dal Titolare o dal Responsabile, i quali devono individuare l'ambito del trattamento consentito a ciascun Incaricato e mantengono, comunque, la diretta autorità sui trattamenti autorizzati.

La nomina deve avvenire con apposita lettera, contenente le direttive e le istruzioni per il trattamento e deve essere controfirmata per accettazione dall'Incaricato.

N.B.: All'atto della nomina deve essere messa a disposizione di ogni Incaricato una copia della disciplina interna di gestione della privacy.
L'Incaricato ne firma l'originale per presa visione sull'apposito foglio firme.
La completa informazione sul presente sistema di gestione, così trasmessa, soddisfa l'obbligo di istruzione da parte del Titolare del trattamento a norma dell'art. 29 Regolamento UE ("*il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali, non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento*").

La nomina a Incaricato del trattamento è a tempo indeterminato, salva cessazione del rapporto di lavoro/servizio dell'Incaricato con **Bioware S.r.l**. ovvero salva la revoca da parte del Titolare/Responsabile.

Il potere di revoca da parte del Titolare può essere esercitato in ogni momento e senza preavviso.

b) L'**Amministratore di sistema** **** ("*provvedimento" del Garante per la protezione dei dati personali del 27 novembre 2008 recepito nella Gazzetta Ufficiale. n. 300 del 24 dicembre 2008) – Sebbene il Regolamento UE 2016/679 non contenga alcun riferimento all'obbligo di nomina dell' Amministratore di Sistema si ritiene che il Provvedimento 27 novembre 2008 sia ancora applicabile per la parte in cui risulta compatibile con le disposizioni del Regolamento UE 2016/679. L'A. di S. può essere infatti considerato una delle "misure di sicurezza" che il Titolare del trattamento , ai sensi dell'art. 32 del Regolamento UE, è tenuto a porre in essere per la miglior tutela dei dati delle persone fisiche*) è il soggetto a cui è conferito il compito di sovrintendere alle risorse tecniche del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione, con il compito altresì di gestire, attribuire

e revocare le credenziali di autenticazione. Tramite le credenziali è possibile costruire il profilo di autorizzazione, cioè la capacità di ogni incaricato di accedere alle proprie cartelle di lavoro, secondo le direttive stabilite dal Titolare del trattamento insieme ai responsabili di area.

Con la definizione di "amministratore di sistema" si individuano generalmente, in ambito informatico, figure professionali finalizzate alla **gestione** e alla **manutenzione** di un impianto di elaborazione o di sue componenti.

Ai fini del presente provvedimento vengono però considerate tali anche altre figure, equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali:

- gli amministratori di basi di dati,
- gli amministratori di reti e di apparati di sicurezza e
- gli amministratori di sistemi software complessi.

Gli amministratori di sistema così ampiamente individuati, pur non essendo preposti ordinariamente a operazioni che implicano una comprensione del dominio applicativo (significato dei dati, formato delle rappresentazioni e semantica delle funzioni), nelle loro consuete attività sono, in molti casi, concretamente "responsabili" di specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati.

Attività tecniche quali il salvataggio dei dati (**backup/recovery**), l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione hardware comportano infatti, in molti casi, un'effettiva capacità di azione su informazioni che va considerata a tutti gli effetti alla stregua di un trattamento di dati personali; ciò, anche quando l'amministratore non consulti "in chiaro" le informazioni medesime.

L'attribuzione della funzione di Amministratore di sistema deve essere preceduta, da parte del Titolare del trattamento, dalla valutazione delle caratteristiche di **esperienza, capacità e affidabilità** del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, compreso il profilo relativo alla sicurezza.
La designazione deve essere individuale, anche in caso di servizi affidati in outsourcing, e deve recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.
La nomina avviene con apposita lettera di incarico presuppone l'esistenza o l'instaurazione di un rapporto di lavoro dipendente o di un rapporto di servizio fra Bioware S.r.l. come Titolare del trattamento e il soggetto designato come amministratore di sistema.

La nomina dell'amministratore di sistema è a tempo indeterminato, salva cessazione del rapporto di lavoro/di servizio con l'amministratore, che comporta automatica decadenza dalle funzioni di amministratore di sistema.

Nel caso di servizi di amministrazione di sistema **affidati in outsourcing** il titolare o il responsabile del trattamento devono conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema. Gli estremi

identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti anche da parte del Garante.
Le attività in outsourcing, ai sensi del Regolamento Ue 2016/679 *necessitano della redazione di un contratto specifico con attribuzione del ruolo di Responsabile esterno del trattamento*.

Qualora l'attività degli amministratori di sistema riguardi anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale di lavoratori (cioè l'amministratore di sistema sia nelle condizioni di acquisire conoscenza di dati a essi riferiti), i titolari pubblici e privati nella qualità di datori di lavoro sono tenuti a rendere nota o conoscibile l'identità degli amministratori di sistema nell'ambito delle proprie organizzazioni, secondo le caratteristiche dell'azienda o del servizio, in relazione ai diversi servizi informatici cui questi sono preposti.
Ciò, avvalendosi:

- dell'informativa resa agli interessati ai sensi dell'art. 13 (e 14) Regolamento UE 2016/679 nell'ambito del rapporto di lavoro che li lega al titolare,
- oppure, tramite il disciplinare tecnico la cui adozione è prevista dal provvedimento del Garante n. 13 del 1° marzo 2007 (in G.U. 10 marzo 2007, n. 58);
- in alternativa, si possono anche utilizzare strumenti di comunicazione interna (a es., intranet aziendale, ordini di servizio a circolazione interna o bollettini).

  - L'operato dell'amministratore di sistema è oggetto, con cadenza almeno annuale, di un'attività di verifica da parte del Titolare o del Responsabile del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

Devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema.

Le registrazioni (**access log**) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste.

Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.

Nell'ipotesi in cui l'amministratore di sistema abbia accesso a dati personali, deve essere dato adeguato adempimento al disposto dell'art. 29 Regolamento UE ("*il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia*

accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri").

Le istruzioni all'Amministratore di sistema sono contenute nella lettera di incarico.

6. TRATTAMENTI DI DATI PERSONALI AFFIDATI ALL'ESTERNO

Il Titolare del Trattamento può decidere di affidare il trattamento dei dati in tutto o in parte all'esterno della propria struttura.
In particolare il Titolare del trattamento può decidere di nominare uno o più **Responsabili del trattamento in outsourcing** ovvero di designare uno o più **Titolari autonomi del trattamento in outsourcing**.

La prima scelta presuppone che:

- il Titolare possa esercitare un potere di indirizzo e di controllo sul soggetto esterno in merito alle modalità del trattamento e alle misure minime di sicurezza da adottare. In questa ipotesi il Responsabile del trattamento in outsourcing è equiparato - quanto a funzioni, responsabilità, valutazione delle competenze e delle conoscenze, modalità di incarico e necessità di verifica periodica dell'operato - a un Responsabile del trattamento.

La seconda scelta è da privilegiare quando:

- il Titolare del trattamento non possa esercitare alcun potere di indirizzo e di controllo nei confronti del soggetto esterno.
  In questo caso il soggetto esterno assume ruolo, funzioni e responsabilità di un autonomo titolare del trattamento, che risponde direttamente e in via esclusiva in proprio della rispondenza alla normativa vigente del trattamento effettuato. In questa ipotesi **Bioware S.r.l.** deve assicurarsi che siano rispettate le norme vigenti in materia di privacy (*rectius*: **corretto trattamento dei dati personali**) ad un livello non inferiore a quanto stabilito per il trattamento interno.
  Ciò avviene attraverso il rilascio da parte del Titolare cui è stato affidato il trattamento dei dati all'esterno di una dichiarazione scritta da cui risulti l'impegno al rispetto della normativa vigente, alla tutela dei diritti in materia di riservatezza dei dati personali e all'adozione delle idonee misure di sicurezza per il trattamento ai sensi del Codice privacy, rispettando le misure minime previste dal Disciplinare tecnico e a quanto prescritto dal Regolamento Ue 2016/679.

Ove uno più trattamenti siano affidati all'esterno deve essere specificato **nell'organigramma della privacy** l'elenco dei soggetti che effettuano il trattamento dei dati in tutto o in parte all'esterno della struttura del titolare, con precisa indicazione per ognuno:
- del tipo di trattamento effettuato
- dei soggetti interessati
- dei luoghi ove avviene il trattamento
- dei soggetti responsabili del trattamento dei dati personali e se si tratta di Responsabili ovvero Titolari

del trattamento in outsourcing

7. TRATTAMENTI DI DATI RACCOLTI DA TERZI

Bioware S.r.l. utilizza per la maggior parte dati raccolti da soggetti Incaricati del trattamento e soggetti al rispetto delle misure di sicurezza stabilite nel presente Manuale e alle verifiche del caso circa la loro concreta adozione.
Può accadere che alcuni dati siano raccolti da soggetti esterni all'organizzazione, in particolare da agenti operanti nell'esercizio del loro mandato professionale.
Gli agenti si considerano responsabili del rispetto della legislazione vigente quanto alla informativa dell'interessato e alla richiesta di consenso per la raccolta, il trattamento e la comunicazione a **Bioware S.r.l.** dei dati stessi.
Il Responsabile del trattamento si accerta del rispetto della suddetta normativa raccogliendo da ogni agente una apposita dichiarazione di impegno.

8. ELENCO DEI TRATTAMENTI E DELLE BANCHE DATI

Bioware S.r.l. svolge attività prevalente di sviluppo, produzione e commercializzazione di prodotti o servizi innovativi ad alto valore tecnologico.
Nello svolgimento della propria attività Bioware S.r.l. tratta i seguenti dati personali per le seguenti finalità:

☐ **dati dei dipendenti** per finalità di gestione del rapporto di lavoro e di organizzazione dell'attività di impresa
☐ **dati di fornitori (agenti in regime di lavoro autonomo, prestatori di beni o servizi, consulenti esterni)** per finalità di gestione del rapporto di prestazione di servizi o di merci, per l'adempimento da parte di Bioware S.r.l. degli obblighi derivanti dal contratto e per finalità contabili e fiscali
☐**dati dei clienti** per finalità di adempimento degli obblighi precontrattuali e contrattuali, per finalità amministrative, contabili e fiscali e per finalità di aggiornamento sulle proposte commerciali
☐ **dati dei soggetti che richiedono informazioni sul sito Internet:** dati non trattenuti.

- Per ciascun trattamento esiste un archivio dei dati trattati, gestito sotto la diretta responsabilità del Titolare del trattamento da parte di uno o più incaricati. Ogni archivio è gestito in parte con modalità elettroniche e in parte con modalità cartacee.
- Per ciascun trattamento è elaborato un registro del trattamento nel quale sono indicati:

a) il nome e i dati di contatto del titolare del trattamento;
b) le finalità del trattamento;
c) le basi giuridiche su cui si basa il trattamento;
d) una descrizione delle categorie di interessati e delle categorie di dati personali trattati;

e) le categorie di attività di trattamento effettuate con il nome e i dati di contatto dei relativi Responsabili (se designati in persona diversa dal Titolare);

f) i soggetti incaricati del trattamento e la descrizione delle operazioni che ciascuno è autorizzato a svolgere (*principio della minimizzazione e separazione accessi e rispetto della "profondità" di accesso)*

g) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;

h) una descrizione generale delle misure di sicurezza tecniche e organizzative adottate;

i) i termini ultimi previsti per la cancellazione delle diverse categorie di dati.

Stando al dato letterale di cui all'art. 30 GDPR e sulla base delle indicazioni del Garante la Bioware S.r.l. ritiene conveniente dotarsi del registro dei trattamenti, in aderenza al principio di *accountability* e di trasparenza.

Il registro dei trattamenti saranno sottoposti a revisione periodica e aggiornati ove necessario dal Titolare del trattamento, in ottica di un processo di miglioramento continuo.

9. MISURE DI SICUREZZA DEI DATI PERSONALI

9.1 Finalità e tipologia

I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi:

a) di distruzione o perdita o modifica, anche accidentale, dei dati stessi

b) di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta

Le misure di sicurezza previste nel presente Manuale comprendono non solo quelle da ritenersi necessarie e comunque di fatto obbligatorie ai sensi del d. lgs. 196/2003 (le c.d. misure minime e idonee ai sensi degli art. 33 ss. del codice) – secondo il testo previgente (che si ritiene doveroso mantenere - comprendenti la legittima conservazione e la sicurezza dei dati trattati), ma anche le misure adeguate messe in atto sulla scorta delle indicazioni contenute nel GDPR (artt. 32-39), quali:

- la valutazione di impatto sulla protezione dei dati,
- il rispetto dei requisiti di autorizzazione preventiva e di consultazione preventiva dell'autorità di controllo e del responsabile della protezione dei dati,
- la designazione del responsabile della protezione dei dati ove applicabile,
- la definizione di informazioni e comunicazioni trasparenti da fornire all'interessato.

Queste ultime misure, ulteriori e integrative, sono alla data di revisione del presente documento ormai obbligatorie pertanto l'azienda le adotta in via definitiva.

Le suddette misure comprendono, se del caso:

a) la pseudonimizzazione e la cifratura dei datipersonali;

b) la **capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità** e la resilienza dei sistemi e dei servizi di trattamento;

c) la **capacità di ripristinare tempestivamente** la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

e) le misure conseguenti ad una eventuale violazione dei dati personali trattati. Con il termine "violazione" si intendono: la *distruzione*/la *perdita*/la *modifica*/la *divulgazione non autorizzata*/*l'accesso non autorizzato* ai dati personali, in maniera illecita o accidentale.

9.2. Analisi dei rischi (valutazione di impatto sulla protezione dei dati)

Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata, dal trattamento non consentito o non conforme alle finalità della raccolta o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati (Art. 32, co. 2 Regolamento UE 2016/679).

Per ciascuna banca dati deve essere predisposta una valutazione dell'impatto sulla sicurezza dei dati personali dei diversi fattori di rischio secondo i seguenti criteri:

A. Classificazione dei rischi in funzione dell'evento che li determina:

- Comportamento degli operatori:
  - *Errore materiale*
  - *Comportamenti sleali e fraudolenti*
  - *Carenza di consapevolezza, ignoranza legislativa o delle procedure, disattenzione*
  - *Sottrazione delle credenziali di autenticazione*
- Eventi relativi agli strumenti:
  - *Azioni di virus informatici o di programmi suscettibili di arrecare danno*
  - *Accessi abusivi al sistema*
- Eventi relativi al contesto:
  - *Accesso non autorizzato a locali/reparti ad accesso limitato*
  - *Sottrazione di strumenti contenenti dati*

B. Descrizione dell'impatto sulla sicurezza (gravità del rischio):

- Bassissimo
- Basso
- Medio/basso
- Medio
- Alto

La valutazione prende in considerazione due fattori: sia la **probabilità** che il rischio di evento dannoso si concretizzi, sia **l'entità dell'evento dannoso** (c.d. magnitudo) nell'ipotesi in cui il rischio dovesse concretizzarsi, soprattutto in relazione alla natura dei dati trattati e al profilo di danno che potrebbe

scaturire.

C. Indicazione delle misure di sicurezza adottate o da adottare, articolate fra:

- Contromisure di carattere fisico:

- *chiusura a chiave armadio;*
- *chiusura a chiave locali;*
- *dotazione di porte blindate*
- *sistema di allarme*

- Contromisure di carattere procedurale:

- *mappatura dei rischi e individuazione delle misure di sicurezza;*
- *istruzione incaricati;*
- *controllo accessi*
- *modifica periodica delle password;*
- *adozione di un regolamento per la gestione del sistema informatico interno;*
- *verifica periodica dell'adozione e dell'efficacia delle misure di sicurezza sulla privacy (**efficace attuazione del modello**)*

- Contromisure di carattere informatico:

- *identificazione utente;*
- *autenticazione utente;*
- *adozione di idonei programmi antivirus e antintrusione*

9.3. Trattamento effettuato con mezzi elettronici

Il trattamento di dati personali effettuato con strumenti elettronici presuppone l'adozione delle seguenti misure minime:

a) *Previsione di un sistema di autenticazione informatica*

Il Titolare, al fine di garantire l'integrità e la disponibilità dei dati, deve adottare dei sistemi che consentano l'accesso agli strumenti elettronici solo a chi è autorizzato. E' introdotto, pertanto, un sistema di autenticazione informatica, definito dal Codice come l'insieme degli strumenti elettronici e delle procedure per la verifica dell'identità del soggetto che tratta, o comunque viene in contatto con, dati personali.
La verifica può avvenire con diverse modalità, ad esempio tramite una tecnica biometrica, dall'iride alle impronte digitali, che individua in modo diretto la persona o anche con modalità indirette mediante un codice, che individua la persona indirettamente, per il fatto che essa lo conosce e lo digita.

b) *Adozione di procedure di gestione delle credenziali di autenticazione*

In correlazione con il punto precedente, sono introdotte procedure di gestione delle credenziali di autenticazione, cioè procedure che consentono di decidere preventivamente con quali modalità i dati e i dispositivi, in possesso di una persona, utilizzati per l'autenticazione informatica, debbano essere usati dall'utente.

- ***Non è ammissibile che i medesimi dati o dispositivi siano conosciuti da, o correlati a,* più persone.**
- ***Le password vengono aggiornate ogni 100 giorni ed è vietato l'utilizzo di password già usate.***

Ogni Incaricato della Società deve essere dotato di credenziali che gli consentono di superare una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.

- **Nel sistema attualmente adottato** da Bioware S.r.l**.** ogni incaricato è dotato di credenziali che gli consentono di superare una procedura di autenticazione per l'accesso e il trattamento dei dati conservati su supporto informatico.

  Le credenziali sono costituite da un codice che identifica l'Incaricato (*username*) e da una parola chiave (*password*) conosciuta solamente dall'incaricato (ogni "utente" ha una sua username e password) che egli stesso provvede:

- ad elaborare,
- mantenere riservata e
- modificare periodicamente.

L'Amministratore di sistema si attiene, nell'attribuzione delle credenziali e nella loro gestione, alle istruzioni ricevute in sede di nomina.

Nel caso in cui l'accesso ai dati e agli strumenti elettronici sia consentito esclusivamente mediante l'uso della componente riservata della credenziale per l'autenticazione, devono essere impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'Incaricato, assenza o impedimento che renda indispensabile e indifferibile intervenire per (N.B.) esclusive necessità di operatività e di sicurezza del sistema.

In genere l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale di autenticazione (password), che l'incaricato provvede ad elaborare e mantenere segreta.

La regola generale è che nessuna persona diversa dall'Incaricato, neppure il Titolare del trattamento, possa accedere allo strumento elettronico, utilizzando la credenziale di autenticazione dell'Incaricato.

Eccezione a tale regola si ha solo se si verificano congiuntamente le seguenti condizioni:

- **prolungata assenza o impedimento dell'incaricato;**
- **l'intervento è indispensabile e indifferibile;**
- **vi sono concrete necessità, di operatività e di sicurezza del sistema**.

L'Amministratore di sistema, quando si trova nelle condizioni sopra illustrate, deve permettere l'accesso ai dati da parte di altri soggetti (che possono essere scelti dall'Incaricato assente o dal Titolare), avvertendo l'Incaricato, se possibile, ovvero avvertendo il sostituto di fornire la descrizione scritta dell'intervento effettuato all'Incaricato al suo rientro.

***c) Utilizzazione di un sistema di autorizzazione*.**

I profili di autorizzazione, per ciascun Incaricato o per classi omogenee di Incaricati, devono essere individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

d) *Aggiornamento periodico dell'individuazione dell'ambito del trattamento* consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici.

Periodicamente, e comunque almeno annualmente, si deve verificare la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.
Nell'ambito di tale aggiornamento periodico si deve conseguentemente provvedere a controllare la lista degli Incaricati, la quale può essere redatta anche per classi omogenee di incarico.

e) *Protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati,* ad accessi non consentiti e a determinati programmi informatici

I dati personali devono essere protetti contro il rischio di intrusione dell'azione di programmi di cui all'art. **615-quinquies** del codice penale mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.

➢ Il primo aspetto - applicazione di antivirus - riguarda la protezione dei dati personali dal rischio di intrusione e dall'azione di programmi di cui all'articolo 615 - quinquies del codice penale, aventi per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento (comunemente conosciuti come virus).

- A tale fine, si è dotati di idonei strumenti elettronici e programmi, che si AGGIORNANO QUOTIDIANAMENTE.

Tutti gli incaricati sono stati istruiti, in merito all'utilizzo dei programmi antivirus e, più in generale, sulle norme di comportamento da tenere, per minimizzare il rischio di essere contagiati: a tale fine, è stato loro distribuito un codice dei comportamenti da tenere, e di quelli da evitare.

Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti devono essere effettuati almeno una volta l'anno. In caso di trattamento di dati sensibili (particolari) o giudiziari l'aggiornamento deve essere fatto almeno semestralmente.
Il Titolare assicura il salvataggio dei dati con frequenza giornaliera.

Ai sensi dell'articolo **615-ter** del codice penale, si ha un accesso abusivo quando ci "*si introduce abusivamente in un sistema informatico o telematico, protetto da misure di sicurezza, ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo*".

➢ Il secondo aspetto - applicazione del firewall - riguarda la protezione degli elaboratori dall'accesso abusivo, di cui all'articolo 615-ter del codice penale, ai sensi del quale compie tale reato chi si introduce abusivamente in un sistema informatico o telematico, protetto da misure di sicurezza, ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo.

Le differenze tra l'ipotesi concernenti programmi virus e simili e quella in esame comportano possibili conseguenze pratiche e sono:

- nell'ipotesi di virus l'intruso è essenzialmente un programma che, per quanto pericoloso possa essere, non indica necessariamente l'esistenza di un attacco criminoso diretto alla società;
- nell'ipotesi in esame, l'intruso è invece una mente con disegno criminoso, che utilizza un determinato programma, per accedere ad un sistema e compiervi azioni illecite (tra le quali, per inciso, vi potrebbe essere il disseminare i programmi contenenti virus).

Considerata la necessità che i dati personali siano protetti anche rispetto a eventuali accessi abusivi da parte dei soggetti autorizzati al trattamento (in particolare lo stesso Amministratore di sistema), devono essere adottati idonei sistemi di registrazione degli accessi logici ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo di tempo non inferiore a sei mesi.

f) *Adozione di procedure per la custodia di copie di sicurezza, il ripristino della* disponibilità dei dati e dei sistemi

Per tutti i dati gestiti sui server deve essere adottato un ***piano di backup***.
Tale piano deve prevedere e garantire il salvataggio giornaliero. Il server deve essere collegato a un gruppo di continuità il quale consenta di escludere la perdita dei dati dovuti a sbalzi di tensione o di interruzione di corrente elettrica.

- **Attualmente**, il backup avviene su due NAS, separati e distinti, posti in due luoghi fisici diversi, che si aggiornano quotidianamente. L'aggiornamento sistemi viene effettuato almeno una volta l'anno, in considerazione del fatto che la natura dei dati trattati non richiede tempistiche necessariamente più ristrette.

g) *Istruzioni organizzative e tecniche per la custodia e l'uso del supporto rimovibile*

In base al Disciplinare Tecnico "i supporti rimovibili contenenti dati di natura particolare o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili".
Si deve dedicare una particolare attenzione ai supporti rimovibili contenenti dati sensibili o giudiziari, nei seguenti termini:

- devono essere custoditi ed utilizzati in modo tale da impedire accessi non autorizzati (furti inclusi) e trattamenti non consentiti;
- i documenti contenenti **dati ultrasensibili/particolari** (segnatamente, i dati relativi alla salute e alle visite mediche dei dipendenti) devono essere custoditi in settori e cartelle separate dagli altri dati, con maggiori misure di sicurezza; gli stessi prevedono l'adozione di misure per garantire accessi minimi e separati solo agli incaricati specificamente dedicati;
- una volta cessate le ragioni per la conservazione dei dati, i supporti non possono venire abbandonati, ma si devono porre in essere gli opportuni accorgimenti, finalizzati a rendere inintelligibili e non ricostruibili tecnicamente i dati in essi contenuti, al fine di impedire che essi possano essere accessibili a persone non autorizzate al trattamento. Si devono quindi cancellare i dati o arrivare addirittura a distruggere il supporto, se necessario.

La copia su supporto rimovibile (floppy disk, cd rom, chiave USB, hard disk esterni) di dati comuni, sensibili e giudiziari da parte degli Incaricati non deve essere possibile. Eventuali autorizzazioni alle copie dovranno essere effettuate ad hoc.

h) *Protezione Strumenti Informatici*

La Società deve provvedere a sensibilizzare tutti gli utenti dei PC a installare solo software autorizzati.
Per software autorizzato si intende software che sia stato valutato dalla Società e quindi adottato per i suoi aspetti di funzionalità e di sicurezza.
Nessun altro software deve essere installato in società, né proveniente da pubblicazioni, né proveniente da Internet.
L'uso da parte delle risorse degli strumenti informatici e telematici forniti dall'azienda è disciplinato in un apposito Regolamento, che è allegato al presente sistema. Le regole ivi stabilite integrano le misure stabilite per la protezione degli strumenti informatici.

i) *Uso di Internet e della posta elettronica*

La Società deve provvedere a stabilire le regole interne di utilizzo di Internet e della posta elettronica aziendale e personale al fine di minimizzare il rischio di contagio del sistema informatico e di garantire la controllabilità di ogni comportamento di gestione dei dati personali trattati, compresa la comunicazione fra Incaricati, all'interessato e a soggetti terzi.

j) *Protezione Locali Server.*

La protezione dei Locali Server è affidata a sistemi fisici e tecnologici logici (chiavi, sistemi antincendio). L'accesso ai locali server, dotate di chiusura a chiave, è consentito solo a personale autorizzato (Responsabile del trattamento dei dati personali, Amministratore di sistema, Incaricato del back up giornaliero dei dati).
Nella sala server sono custoditi in un'apposita cassetta, a propria volta munita di chiusura tramite chiave, i supporti su cui sono registrati i dati della Società nel back up quotidiano.

Devono essere previsti i necessari dispositivi di sicurezza indicati dal D.Lgs 81/08, quali rivelatori di calore, campanelli di allarme in caso di incendio, estintori di incendio, uscite di sicurezza.

9.4. Trattamento effettuato con mezzi non elettronici

Il trattamento di dati personali senza l'ausilio di strumenti elettronici è effettuato adottando le seguenti misure minime:

a) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;
b) protezione degli uffici e dei locali ove si trattano dati in forma non elettronica
c) previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;
d) previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.

a) Aggiornamento periodico dell'individuazione dell'ambito del trattamento **consentito ai singoli incaricati o alle unità organizzative:** periodica revisione di tali ambiti.

b) protezione degli uffici e dei locali ove si trattano dati in forma non elettronica:

I locali della Società sono situati in quartieri a basso tasso di criminalità, non si sono registrati intrusioni o tentativi di intrusione negli ultimi 5 anni. Ciascun dipendente provvede prima dell'uscita alla chiusura delle finestre, allo spegnimento delle luci; l'incaricato provvede alla chiusura delle porte d'ingresso e all'attivazione dei sistemi di allarme, ove esistenti.
L'accesso ai locali dell'azienda è controllato.
Le porte di ingresso rimangono chiuse anche durante l'orario di lavoro. Il personale provvede a identificare i terzi estranei e a consentire l'accesso solo alle persone autorizzate. I terzi estranei attendono di essere ricevuti nella apposita sala e, al di fuori, sono costantemente accompagnati dal personale.
I tavoli di lavoro degli Incaricati sono collocati in stanze chiuse da porte con serratura, alle quali è consentito l'accesso solo alle persone autorizzate o in compagnia delle stesse. In ogni caso ciascun Incaricato cura di non lasciare documenti contenenti dati personali in vista di terzi e di custodire in armadi chiusi a chiave cartelle o supporti rimovibili contenti dati sensibili o comunque riservati.
Stampanti ed apparecchi telefax sono ubicati in modo che nessun estraneo possa leggere od asportare eventualmente documenti non ancora prelevati dall'incaricato.
Durante la chiusura degli uffici e del magazzino i locali sono presidiati da antifurto.

c) procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo **svolgimento dei relativi compiti:**

La protezione degli uffici è assicurata con le stesse modalità previste per i locali server nel rispetto di quanto indicato dal D.Lgs 81/08.
Il Titolare o il Responsabile, se nominato, ove lo ritenga necessario per meglio proteggere la sicurezza degli uffici e degli archivi cartacei, può limitare l'accesso degli Incaricati ai soli dati personali la cui

conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati.
In pratica si permette l'accesso ai soli atti e documenti che siano contenuti in archivi ad accesso selezionato. Per archivi ad accesso selezionato si intendono quegli archivi che non sono disponibili a tutti, cioè gli archivi ai quali si possa accedere mediante una modalità preventivamente individuata. Tali modalità possono essere le seguenti a scelta:

- fornire la chiave dell'archivio ai soli soggetti autorizzati;
- permettere l'estrazione dei documenti solo dopo la registrazione dei nominativi in un apposito registro accessi.

N.B.: Tale misura viene adottata a maggior ragione per gli archivi contenenti dati sensibili: in particolare, tali dati devono essere conservati in armadi muniti di serratura ai quali è autorizzato l'accesso solo al Medico competente (per le cartelle sanitarie necessarie per la sorveglianza sanitaria) e agli Incaricati autorizzati al trattamento dei dati dei dipendenti (per i dati sensibili eventualmente raccolti dai dipendenti). I dati comuni memorizzati su supporti cartacei sono conservati in armadi ad accesso selezionato, ai quali accede l'Incaricato adibito al trattamento dei dati ivi contenuti.
Gli armadi devono essere chiusi al termine dell'orario di lavoro al fine di impedire l'accesso ai soggetti non autorizzati che per ragioni di manutenzione o pulizia dei locali possano trovarsi a essere fisicamente presenti negli Uffici.
In ogni caso, le aree contenenti archivi sono ubicate in modo tale che ciascun addetto possa rilevare a vista il tentativo di accesso da parte di persone estranee.
A protezione degli archivi cartacei devono essere attivati i necessari dispositivi di sicurezza quali rivelatori di fumo o di calore, campanelli di allarme in caso di incendio, estintori di incendio. Bioware S.r.l. è regolarmente prevista degli estintori necessari secondo il piano di emergenza allegato al DVR. Gli estintori sono regolarmente mantenuti.

9.5. Elenco delle sedi e degli uffici dove vengono trattati i dati personali

Sede Legale	Bioware S.r.l. Via di Vannina 88, 00156 Roma (RM)	
Uffici		**Tipo di accesso** CONTROLLATO Esiste una chiusura con serratura; l'accesso è consentito solo alle persone autorizzate, munite della apposita chiave
Sede Operativa	Zona Industriale Mazzocchio II 04014 Pontinia (LT)	
Uffici		CONTROLLATO

9.6. Misure conseguenti ad una eventuale violazione dei dati personali trattati (c.d. *data breach*)

In caso di violazione dei dati personali, il designato interno nel ruolo di Responsabile del trattamento, ove nominato, ovvero l'Incaricato che per primo ne venga a conoscenza informa il Titolare del trattamento senza ingiustificato ritardo.

Il Titolare del trattamento, a sua volta, notifica la violazione all'autorità garante senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne sia stato informato. Qualora non sia effettuata entro 72 ore, la notifica all'autorità di controllo è corredata dei motivi del ritardo.
(**N.B.: nel caso di nomina di uno o più Responsabili in outsourcing il contratto dovrà prevedere espressamente l'obbligo di questi di comunicazione della violazione al Titolare entro termini brevi, al fine di poter rispettare il termine di 72 ore previsto)**.
La notifica non è necessaria qualora il Titolare del trattamento, consultato il Responsabile della protezione dei dati personali (ove nominato), valuti improbabile che la violazione avvenuta presenti un rischio per i diritti e le libertà delle persone fisiche.

La notifica deve:

a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c) descrivere le probabili conseguenze della violazione dei dati personali;
d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Il Responsabile del trattamento documenta ogni eventuale violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto dell'obbligo di notifica.

La procedura attualmente praticata prevede:

- il blocco del sistema da parte dell'Amministratore di sistema;
- la pulizia del sistema;
- il ripristino di tutti i dati di back up.

9.7. Formazione del personale

Bioware S.r.l. promuove la formazione del proprio personale dipendente in materia di

privacy attraverso la consegna di dettagliate istruzioni scritte a coloro che assumono il ruolo di Incaricati del trattamento di dati personali e la messa a disposizione del presente Manuale di sistema.
Il Titolare del trattamento (ovvero il Responsabile del trattamento, ove nominato) valuta all'atto della

nomina di ciascun Incaricato al trattamento di dati personali, sulla base dell'esperienza e delle specifiche conoscenze da costui possedute, la necessità di un intervento di formazione, riguardante la normativa vigente e la disciplina interna in materia di privacy, i rischi che incombono sui dati, le misure disponibili per prevenire eventi dannosi, l'esecuzione dei propri compiti e le relative responsabilità.

Il Titolare del trattamento (ovvero il Responsabile del trattamento, ove nominato), inoltre, valuta in sede di revisione periodica annuale la necessità di interventi formativi di aggiornamento in relazione a variazioni del sistema, novità normative o altre specifiche esigenze.

10. GESTIONE DEL SITO INTERNET

Bioware S.r.l. è dotata di un sito Internet aziendale.
Il sito ha carattere prevalentemente informativo, tuttavia alcuni aspetti sono rilevanti sotto il profilo della riservatezza dei dati personali.

a) Il sito deve ospitare, in una sezione visibile ad ogni utente, l'esposizione della privacy policy con riferimento a ogni aspetto suscettibile di essere assimilato a una raccolta e a un trattamento di dati personali (quantomeno con riferimento all'utilizzo dei cookies).
b) Sul sito non dovranno in generale comparire dati e immagini, né tramite il sito dovranno essere raccolti dati senza la preventiva autorizzazione dei soggetti interessati.
   La gestione e manutenzione del sito è affidata a società esterna che agisce in qualità di responsabile in outsourcing.

11. CONSERVAZIONE DEI DATI

Il periodo di conservazione dei dati sia informatici sia cartacei è, per alcuni casi, imposto dalle normative vigenti (5/10 anni, ad es. libro unico del lavoro, fatture, ecc.).
In altri casi il dato deve essere conservato solo per il periodo in cui il trattamento viene effettivamente svolto.
I dati possono essere cancellati quando la conservazione degli stessi non sia più necessaria agli scopi per i quali essi sono stati raccolti e successivamente trattati.
I dati devono essere distrutti con sistemi meccanici o automatizzati che non ne prevedano in alcun modo il recupero. I dati possono altresì essere cancellati su richiesta dell'interessato sempre che la loro conservazione non sia necessaria per legge né che sia indispensabile per singole frazioni di trattamento.

12. EVASIONE DELLE RICHIESTE DI ACCESSO, DI CANCELLAZIONE DI OPPOSIZIONE DELL'INTERESSATO

Il Codice/Regolamento UE 2016/679 dopo aver delineato i principi generali che regolano la protezione dei dati personali, ha individuato nel titolo II i diritti dell'interessato: tali diritti possono sostanzialmente distinguersi in diritti di conoscenza, diritti di accesso, diritti di intervento e diritti di opposizione.

Per interessato si intende la persona fisica (la persona giuridica, l'ente o l'associazione, nei casi previsti) cui si riferiscono i dati personali.

12.1. I diritti che possono essere esercitati dall'interessato

I diritti che l'interessato può esercitare si possono suddividere in tre categorie:

- il diritto di conoscere quali dati personali sul proprio conto il titolare possieda;
- il diritto di controllare tali dati;
- il diritto di resistere ed opporsi al trattamento, in tutto o in parte.

a) Il diritto di conoscere

L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile. L'interessato ha il diritto di rivolgersi, al titolare o al responsabile, per chiedere se esistano o meno dati personali che lo riguardano. È un diritto che può essere esercitato nei confronti di qualsiasi soggetto che tratti dati personali, anche in mancanza di prova che tale soggetto possegga dati personali di chi esercita il diritto di accesso.
Secondo quanto disposto dall'art. 7, da 15 a 22 e (77) del Regolamento UE 2016/679, l'interessato ha diritto ad ottenere l'indicazione:

- dell'esistenza di dati personali;
- dell'origine dei dati personali;
- delle finalità e modalità di trattamento;
- della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
- degli estremi identificativi del Titolare, dei Responsabili e del rappresentante designato ai sensi (nel caso di trattamento dei dati effettuati all'estero).

La richiesta di accesso di un soggetto interessato può essere rinnovata.

Cosa può chiedere l'interessato?

L'interessato può chiedere la "conferma dell'esistenza o meno dei dati personali che lo riguardano, anche se non ancora registrati" e la loro "comunicazione in forma intelligibile". L'interessato non deve motivare la sua domanda, né è tenuto a circoscrivere l'ambito della propria richiesta, per cui può anche esigere di essere messo al corrente di tutti i trattamenti dei propri dati personali, posti in essere dal Titolare.
Per ottemperare correttamente ad una richiesta non è quindi sempre sufficiente una semplice verifica informatica, ma può divenire necessario esaminare anche il materiale cartaceo, per accertare se esistano o meno dati personali che riguardano chi ha inoltrato la richiesta.
Al soggetto interessato vanno fornite le indicazioni sui dati personali trattati nella ampia accezione di tale termine. Non ci si può limitare a rispondere in termini generici (es. trattiamo alcuni dati anagrafici sul Suo conto, oppure disponiamo di alcuni dati sui Suoi consumi), ma si devono esattamente indicare quali siano i dati anagrafici (es. Nome: Pietro; Cognome: Rossi; Indirizzo: Via delle Nazioni – Milano, telefono 027777777 e-mail: pietrorossi@tin.it) e quali siano le altre informazioni che lo riguardano. Per dato personale, infatti, si intende ogni informazione su un soggetto identificato o identificabile, a prescindere:

- dal supporto che contiene l'informazione: all'interessato dovranno quindi essere rese note non solo le informazioni scritte contenute nell'ambito di documenti cartacei o di supporti elettronici, ma anche le eventuali immagini;
- dalla natura dell'informazione, sia essa di carattere oggettivo oppure di carattere soggettivo

(frutto cioè di giudizi e valutazioni, anche espresse dal Titolare del trattamento).

Per soddisfare in modo conforme alla disciplina di settore la richiesta dell'interessato, non ci si può limitare a fornire l'elenco dei dati trattati, ma si deve anche precisare:

- quale sia l'origine dei dati;
- quali siano le modalità e le finalità su cui si basa il trattamento;
- in caso di trattamento effettuato con l'ausilio di strumenti elettronici, quale sia la logica applicata al trattamento;
- gli estremi identificativi del Titolare e dei Responsabili;
- i soggetti, o le categorie di soggetti, ai quali i dati personali possono essere comunicati;
- i soggetti, o le categorie di soggetti, che possono venire a conoscenza dei dati, in qualità di rappresentante designato nel territorio dello Stato, di responsabili o di Incaricati.

Il Titolare del trattamento, una volta interpellato, non può rifiutarsi di fornire le suddette informazioni, se richiestegli dall'interessato, adducendo il fatto di avere provveduto a cancellare ogni dato personale che si riferisce allo stesso.

b) Il diritto di controllare

L'accesso è finalizzato, oltre che ad accertare quali siano i propri dati che vengono da altri trattati, anche ad ottenere una serie di adempimenti, da parte di chi tratta i dati, che pongano rimedio all'eventuale inesattezza dei dati stessi. L'interessato ha il diritto di chiedere ed ottenere:

- l'aggiornamento e la rettificazione dei dati, qualora essi siano inesatti;
- la loro integrazione, qualora vi abbia interesse.

Ad ulteriore tutela del soggetto interessato, la legge prevede che il Titolare debba comunicare l'aggiornamento, la rettifica o l'integrazione a coloro ai quali i dati sono stati comunicati o diffusi, attestando di avere adempiuto a tale incombenza. Tale operazione può essere evitata solo nel caso in cui tale adempimento si riveli impossibile, o comporti un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

c) Il diritto di opposizione

L'interessato, inoltre, ha il diritto di opporsi, in tutto o in parte, per motivi legittimi al trattamento, potendo altresì richiedere sempre, per motivi legittimi, la cancellazione (diritto all'oblio art. 17 Regolamento UE), la trasformazione in forma anonima o il blocco dei dati.

Il diritto di opporsi non è riferito soltanto ai trattamenti illeciti di dati personali (nel quale caso è ammesso senza alcuna condizione), ma si può esercitare anche nei confronti di trattamenti leciti, pertinenti allo scopo della raccolta. In tali casi l'interessato deve però avere un motivo legittimo per opporsi. Nella concreta valutazione della legittimità del motivo assumono un rilievo decisivo gli interessi ed il comportamento dei soggetti coinvolti. Si può ad esempio giudicare motivo non legittimo, quello di un soggetto che abbia spontaneamente fornito i dati e poi, senza un motivo oggettivamente apprezzabile, voglia ritirarli per il puro gusto di creare un disagio alla banca dati. L'interessato ha, altresì, il diritto di opporsi (in tutto o in parte) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o comunicazione commerciale (art. 7, par. 4, lett. b Codice (abrogato) art. 21 e 21 comma 2 Regolamento UE). L'esercizio di tale diritto è comunque limitato o impedito in alcuni casi (cfr. d. lgs. 101/2018)

12.2. Modalità di esercizio dei diritti da parte dell'interessato

L'interessato può rivolgersi al Garante (anche attraverso il sito internet dedicato) con un reclamo circostanziato (art. 22 e 77 del Regolamento UE 2016/679 nonché art. 140 bis e 141 e ss del Codice come modificato dal D. Lgs. 101/2018) o un ricorso all'autorità giudiziaria qualora ritenga che i diritti di cui gode siano stati violati.
Chiunque può altresì rivolgere segnalazioni al Garante (art. 144 del Codice) allo scopo di rappresentare una violazione della disciplina in materia di dati personali.
L'interessato può rivolgere senza particolari formalità (ad esempio lettera raccomandata, telefax o posta elettronica) la propria richiesta al Titolare o al Responsabile, anche per il tramite di un incaricato del soggetto che tratta i dati personali: ad esempio, nel corso di una telefonata si può richiedere direttamente all'impiegato dell'impresa con cui si è in contatto di avere accesso ai propri dati personali. Sarà compito dell'Incaricato annotare sinteticamente gli estremi della richiesta, consegnandoli successivamente alla persona o all'ufficio che hanno il compito di dare riscontro al soggetto interessato.
Bioware S.r.l. tiene in ogni caso a disposizione degli interessati, e consegna su richiesta degli stessi, un facsimile per l'esercizio dei diritti previsti dall'art. 7 e da 15 a 22 Regolamento Ue 2016/679 (**Modello per l'esercizio dei diritti da parte dell'interessato in materia di privacy**).

La norma prevede che l'interessato debba dimostrare la propria identità, sulla base di idonei elementi di valutazione, anche mediante atti o documenti disponibili o esibendo il documento di riconoscimento ovvero allegando copia dello stesso se la richiesta è inoltrata via posta o con mezzi analoghi.
Vi sono dei casi, tuttavia, nei quali i diritti di cui sopra non possono essere esercitati con richiesta al Titolare e al Responsabile o con ricorso: si tratta dei casi in cui i dati personali siano trattati in base alle disposizioni in materia di riciclaggio, di sostegno alle vittime delle richieste estorsive, di Commissioni parlamentari d'inchiesta; siano trattati da un soggetto pubblico per esclusive finalità inerenti la politica monetaria e valutaria, al sistema dei pagamenti, al controllo degli intermediari e dei mercati creditizi e finanziari, nonché alla tutela della loro stabilità; siano trattati da fornitori di servizi di comunicazione elettronica accessibili al pubblico relativamente a comunicazioni telefoniche in entrata; siano trattati per ragioni di giustizia; siano necessari per lo svolgimento delle investigazioni difensive o per l'esercizio del diritto in sede giudiziaria (limitatamente al periodo durante il quale potrebbe derivarne un pregiudizio effettivo e concreto).

12.3. La risposta all'interessato

Il riscontro alla richiesta, da parte del Titolare o del Responsabile, deve essere in genere fornito entro **un mese**; nei casi più complessi è prevista una proroga di ulteriori due mesi – previsione del Regolamento UE).
Nel caso in cui le operazioni necessarie per un integrale riscontro alla richiesta siano di particolare complessità, ovvero ricorra altro giustificato motivo, il Titolare può informare di tali circostanze l'interessato, entro un mese dal ricevimento della richiesta. La modalità più idonea, per fornire i dati all'interessato consiste nella loro estrazione e nella successiva comunicazione al richiedente, comunicazione che può avvenire anche oralmente, ovvero mediante mezzi elettronici o comunque

automatizzati.
Se vi è richiesta, da parte dell'interessato, si deve provvedere alla trasposizione dei dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica.
Le informazioni devono essere rese in modo tale da rendere agevole la loro comprensione. Di norma vanno quindi fornite solo le informazioni, non i documenti di cui queste sono parte, o i supporti in cui esse sono contenute. L'interessato non può pretendere di ottenere una copia di tutti i documenti in cui vi sono dati personali a lui riferiti
Nei soli casi in cui risulti particolarmente difficoltosa l'estrazione dei dati dai documenti e la loro trasposizione su supporto cartaceo o informatico, il soggetto che tratta i dati può consegnare all'interessato una copia dei supporti in cui essi sono contenuti, a condizione che la consultazione di tale copia consenta ugualmente un'agevole comprensione dei dati personali richiesti, considerata anche la qualità e quantità delle informazioni.
D'altra parte, l'interessato non può pretendere di ottenere una copia, se i dati personali possono venire a lui comunicati in modo esaustivo con il procedimento di estrazione.
Il diritto dell'interessato viene esercitato GRATUITAMENTE: tuttavia, in casi complessi, il Titolare può chiedere un contributo spese all'interessato, che non sia eccedente i costi effettivamente sopportati per la ricerca nel caso specifico, contributo che può essere corrisposto mediante versamento postale o bancario, mediante carta di pagamento o di credito, ove possibile all'atto di ricezione del riscontro e, comunque, non oltre quindici giorni da tale riscontro.

12.4. L'informativa all'interessato sui suoi diritti (artt. 12, 13 e 14 Regolamento UE)

A norma dell'art.13/14 del Regolamento UE, a seconda che la raccolta dati avvenga presso l'interessato o presso terzi, l'interessato o la persona presso la quale sono raccolti i dati personali devono essere previamente informati oralmente o per iscritto circa:

a) le finalità e le modalità del trattamento cui sono destinati i dati;

b) la natura obbligatoria o facoltativa del conferimento dei dati e le basi giuridiche che rendono lecito il trattamento;

c) le conseguenze di un eventuale rifiuto di conferimento;

d) i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;

e) i diritti di cui all'articolo da 15 a 22;

f) gli estremi identificativi del titolare e, se designato, del responsabile interno;

g) il nominativo e il contatto del DPO (se nominato);

h) eventuali attività di profilazione;

i) Se i dati vengono trattati in paesi esteri (UE) o extraUE.

In adempimento di tale obbligo, la **Bioware S.r.l.** ha predisposto:

- l'informativa scritta ai dipendenti, da far sottoscrivere all'atto dell'assunzione contestualmente alla stipulazione del rapporto di lavoro. Nello stesso modulo è presente la formula per la richiesta di consenso al trattamento dei dati, per quanto necessario.
- l'informativa scritta ai clienti e fornitori, da far sottoscrivere all'atto della stipulazione del relativo contratto o, se necessario, all'atto della instaurazione delle trattative precontrattuali (quando l'instaurazione delle trattative implica la raccolta e il trattamento di dati personali di persone fisiche – anche persone giuridiche solo nei casi di cui alla Direttiva 2002). Nello stesso modulo è presente la formula per la richiesta di consenso al trattamento dei dati, per quanto necessario.

Si precisa che l'informativa all'interessato è obbligatoria anche quando i dati sono trattati in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria. Nello stesso caso il trattamento può essere effettuato a prescindere dal consenso dell'interessato.

Potranno pertanto essere senz'altro acquisiti e trattati senza ulteriori adempimenti, fra l'altro, i dati di natura fiscale necessari esclusivamente per adempiere ad obblighi di legge (essenzialmente i dati di natura fiscale contenuti in fatture, ricevute, scontrini da inserire in contabilità).

13. ILLECITI E SANZIONI

Le violazioni alle regole interne in materia di privacy da parte degli Incaricati del trattamento di dati personali potranno essere valutate come illeciti disciplinari ed essere come tali sanzionate.
Poiché le disposizioni contenute nel presente sistema integrano il modello organizzativo aziendale ai sensi del d. lgs. 231/2001, le violazioni a dette disposizioni potranno essere altresì valutate come violazioni al modello organizzativo.
La relativa notizia, pertanto, dovrà essere trasmessa all'ODV per l'assunzione delle conseguenti determinazioni.

14. VERIFICHE E AGGIORNAMENTI

14.1. Verifica periodica del sistema di sicurezza

Il Titolare del trattamento, eventualmente tramite il Responsabile, se nominato, e tramite l'Amministratore di sistema ove necessario, effettua verifiche periodiche del sistema di sicurezza allo scopo di garantirne l'efficacia.

La verifica deve essere effettuata con cadenza almeno annuale e deve essere documentata attraverso un rapporto redatto da conservarsi a cura del Titolare del trattamento (o del Responsabile, ove nominato).
La verifica si svolge mediante analisi delle principali aree di rischio che si elencano di seguito:

- L'accesso fisico ai locali ove si svolge il trattamento automatizzato;
- La gestione delle parole chiave e dei profili di accesso degli Incaricati;
- Le procedure atte a verificare l'integrità e l'aggiornamento dei dati personali;
- La sicurezza delle trasmissioni in rete;
- Le modalità di conservazione dei documenti non soggetti a trattamento automatizzato;
- Le modalità di reimpiego di supporti di memorizzazione
- Il livello di formazione e il grado di apprendimento degli Incaricati.

La verifica, inoltre, dovrà essere finalizzata:
- a garantire la costante rispondenza del presente sistema di gestione della privacy alla normativa vigente. In particolar modo, nel biennio 2018 e 2019 dovrà essere monitorata l'adeguatezza del sistema a ogni ulteriore adempimento o regola introdotti in sede di normazione europea o nazionale in attuazione del Regolamento UE sulla privacy.
- a garantire la costante rispondenza del presente sistema di gestione della privacy alla realtà organizzativa aziendale.

La Società può valutare l'opportunità di effettuare le necessarie verifiche in materia dei dati personali anche ricorrendo a servizi di auditing da parte di studi legali o di società informatiche specializzate.

La verifica periodica circa l'attuazione e l'efficacia del sistema di gestione della privacy rappresenta misura di sicurezza prioritaria, di tipo procedurale, ai fini della tutela della riservatezza dei dati trattati.

14.2. Aggiornamento della documentazione del sistema di protezione dei dati personali

Il presente manuale del sistema di gestione del trattamento dei dati personali, compreso ogni suo allegato, sarà aggiornato a seguito di ogni verifica che riscontri cambiamenti significativi nella struttura del sistema di protezione dei dati personali.

Roma, 23 novembre 2020

Per Bioware S.r.l.
Rappresentante Legale, Massimiliano Barletta

FOGLI FIRME

Io sottoscritto dichiaro che mi è stata messa a disposizione dal Titolare del trattamento versione integrale del Manuale del sistema di gestione del trattamento dei dati personali di Bioware S.r.l.

Copia integrale del Manuale è consultabile presso l'Ufficio del Responsabile del trattamento durante l'orario di lavoro, a semplice richiesta.

Il Titolare del Trattamento non si opporrà alla consultazione del Manuale da parte del Responsabile del trattamento o degli Incaricati, salvo che si tratti di richiesta palesemente ingiustificata o pretestuosa.

ELENCO FIRME

1) Nome e cognome

FIRMA_____

2) Nome e cognome

FIRMA_____

3) Nome e cognome

FIRMA_____

4) Nome e cognome

FIRMA_____

5) Nome e cognome

FIRMA_____

6) Nome e cognome

FIRMA_____

7) Nome e cognome

FIRMA_____

8) Nome e cognome

FIRMA_____

9) Nome e cognome

FIRMA_____

10) Nome e cognome

FIRMA_____

11) Nome e cognome

FIRMA_____

12) Nome e cognome

FIRMA_____